(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－124892
（P2000－124892A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/14		H04L 9/00	641	5B089
G06F	13/00	351	G06F 13/00	351G	5J104
G09C	1/00	660	G09C 1/00	660G	5K030
H04L	9/08		H04L 9/00	601A	
	12/54			601E	

審査請求　有　請求項の数11　ＯＬ　（全　７　頁）　最終頁に続く

(21)出願番号　特願平10－294765

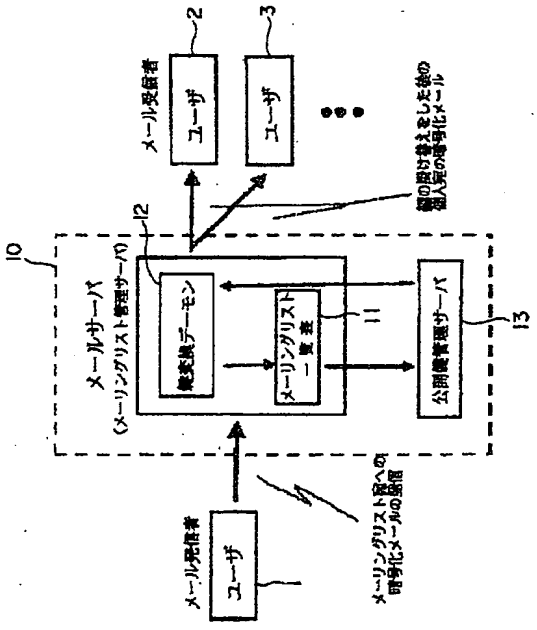
(22)出願日　平成10年10月16日(1998.10.16)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　財津　秀司
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100089875
弁理士　野田　茂

最終頁に続く

(54)【発明の名称】　セキュアメーリングリスト配信方法および装置

(57)【要約】
【課題】　メール送信者は、メールサーバの公開鍵さえ入手すれば、メール受信者の数に無関係にメーリングリスト一覧表の運用を容易に行えるセキュアメーリングリスト配信装置を提供すること。
【解決手段】　メールサーバ１０で管理されるメーリングリスト一覧表１１にユーザ１～３を登録し、ユーザ１がメーリングリスト一覧表１１に暗号化メールを発信すると、鍵変換デーモン１２がユーザ１のメールアドレスと公開鍵を検索して取得する。また、ユーザ１からのメーリングリスト一覧表宛ての暗号化メールをメールサーバ１０の秘密鍵で共通鍵を解読し、共通鍵をユーザ２の公開鍵で再度暗号化してユーザ２に暗号化メールを送信し、ユーザ２は暗号化メールを自己の秘密鍵を用いて複号化する。



【特許請求の範囲】

【請求項１】　メール本文を使用してメール送信者の電子署名を作成して上記メール本文と電子署名をまとめて共通鍵を使用することにより暗号文を作成するとともに、この共通鍵をメール受信者の公開鍵で暗号化する第１ステップと、上記メール送信者より上記メール受信者に送信された上記暗号化された共通鍵をメール受信者の秘密鍵で復号化するとともに、上記暗号化されたメール本文を復号化された共通鍵により復号化する第２ステップと、

上記送信された電子署名を上記メール送信者の公開鍵を用いて復号化するとともに、上記メール本文からメッセージダイジェストを作成する第３ステップと、

メーリングリスト一覧表に登録されているユーザのメールアドレスを鍵変換デーモンによりメーリングリスト一覧表から取得し、その取得したメールアドレスから公開鍵を取得して、このメールアドレスと公開鍵を使用して共通鍵を暗号化する第４ステップと、

を備えることを特徴とするセキュアメーリングリスト配信方法。

【請求項２】　上記メール本文の暗号化は、共通鍵を使用することを特徴とする請求項１記載のセキュアメーリングリスト配信方法。

【請求項３】　上記メール送信者側から送信された上記メール受信者側における電子署名は、公開鍵を使用してメッセージダイジェストを復号化することを特徴とする請求項１または２記載のセキュアメーリングリスト配信方法。

【請求項４】　上記メール送信者側から送信された上記メール受信者側におけるメール本文は、ハッシュ関数を使用してメッセージダイジェストを作成することを特徴とする請求項１、２または３記載のセキュアメーリングリスト配信方法。

【請求項５】　上記鍵変換デーモンは、上記取得したメールアドレスから公開鍵情報管理サーバにより公開鍵を取得することを特徴とする請求項１乃至４に何れか１項記載のセキュアメーリングリスト配信方法。

【請求項６】　上記メール送信側における電子署名の作成は、ハッシュ関数を使用して上記メール本文からメッセージダイジェストを作成することを特徴とする請求項１乃至５に何れか１項記載のセキュアメーリングリスト配信方法。

【請求項７】　上記メッセージダイジェストは、上記メール送信者の秘密鍵で暗号化を行うことを特徴とする請求項６記載のセキュアメーリングリスト配信方法。

【請求項８】　上記鍵変換デーモンは、上記メーリングリスト一覧表に所属している人の公開鍵を一括検索して上記メーリングリスト一覧表に所属している人の公開鍵をまとめて入手することを特徴とする請求項１乃至４に何れか１項記載のセキュアメーリングリスト配信方法。

【請求項９】　上記鍵変換デーモンは、上記メーリングリスト一覧表に所属している人全員の公開鍵をメールとともに送信することを特徴とする請求項１乃至４に何れか１項記載のセキュアメーリングリスト配信方法。

【請求項１０】　複数のユーザを登録したメールリングリストを管理するメールサーバと、

上記メールサーバに存在する公開鍵管理サーバと、

上記メーリングリスト一覧表に登録される上記複数のユーザのうちの所定のユーザがメール送信者となって上記メーリングリスト一覧表宛に登録する暗号化メールの発信時に上記メーリングリスト一覧表に登録されている上記ユーザのメールアドレスと公開鍵を検索して、メールアドレスと公開鍵を取得するとともに、上記メールサーバの秘密鍵で一時的に共通鍵で再度暗号化して上記複数のユーザが暗号化メールを復号化するために上記複数のユーザに暗号化メールを送信する鍵変換デーモンと、

を備えることを特徴とするセキュアメーリングリスト配信装置。

【請求項１１】　上記鍵変換デーモンは、上記メーリングリスト一覧表に登録されている上記ユーザのアドレスと公開鍵の検索を行って必要に応じて公開鍵管理に問い合わせて上記ユーザのアドレスと公開鍵を取得することを特徴とする請求項１０記載のセキュアメーリングリスト配信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、メーリングリスト一覧表を管理しているメールサーバが、メーリングリスト一覧表宛に送られてきた暗号化メールに対して、メーリングリスト一覧表の登録者のメールアドレスと公開鍵を検索し、暗号化メールの鍵のかけかえを行うことにより、メールを発信する人がメーリングリスト一覧表に所属する人の公開鍵を取得していなくても、現実的にメーリングリスト一覧表の運用を可能にしたセキュアメーリングリスト配信方法および装置に関する。

【０００２】

【従来の技術】情報処理技術と通信技術の高速な進展に伴い、通信網を利用して種々の情報を高速かつ安価に送受信することが可能になってきている。このような通信網を利用して、秘密情報の伝送を行うことも重要な課題になっており、秘密情報の伝送量も漸増する状況下にある。

【０００３】そこで、たとえば、特開平０６－１５２５９２号公報には、送信側は平文をデータ鍵で暗号化し、そのデータ鍵と受信者を特定する宛先情報とシステムで共通のマスタ鍵とに基づいて暗号分鍵を生成し、宛先情報と暗号文鍵とに基づいて暗号文鍵を生成し、宛先情報と暗号文鍵と暗号文とからなる通信文を通信網に送出する。受信側では、通信網から通信文を受信し、受信した通信文に含まれる宛先情報と暗号文鍵とからマスタ鍵を

用いてデータ鍵を生成し、そのデータ鍵を暗号文を復号して平文を生成することが開示されている。

【０００４】また、電子メールの送信者と受信者以外の第３者が暗号化電子メールに関する情報管理を行う電子メール暗号化装置が、特開平０９－４６３３０号公報に開示されている。この公報の場合は、所定の暗号鍵を用いて、共通鍵暗号方式により暗号化した電子メールの本文に、この電子メールの送信者と受信者用のそれぞれの公開鍵を用いて、公開鍵暗号方式により暗号化した所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、予め定められた電子メール受信者と送信者以外の第３者の公開鍵を用いて所定の暗号化鍵を暗号化し、第３者の公開鍵により暗号化した所定の暗号鍵を電子メールに付加することが開示されている。

【０００５】上位概念では、このような電子メールの暗号化装置の技術思想の範疇に属する従来の暗号化メールシステムの場合には、電子メール送信者から電子メール受信者に暗号化メールの送信を行う場合には、１対１で行われている。１人の電子メール送信者から複数（ｎ人）の電子メール受信者に暗号化メールの送信を行う場合には、１対１×ｎ回暗号化メールを電子メール送信者から電子メール受信者に発行しなければならない。

【０００６】

【発明が解決しようとする課題】しかしながら、このような暗号化メールシステムの場合には、暗号化メールを発行する側が複数の人の公開鍵を知る必要があり、通常の暗号化メールシステムで使用されるメーリングリスト方式を使用することができない。さらに、近時メーリングリスト一覧表への登録者が増え、しかも、メール自体も付加価値のつく内容のものが含まれているために、暗号化メールを使用するようになってきている。

【０００７】しかるに、現状では、暗号化メールの場合、クライアント側で１００人なら１００人のそれぞれの公開鍵を入手して、その公開鍵からそれぞれの人に対して暗号化メールを送るようになっている。したがって、このような暗号化メールの場合では、現実的な運用ができず、また、公開鍵も変更された場合などを勘案すると、より非現実的になり、このような課題を解決する方策が望まれていた。

【０００８】この発明は、上記従来の課題を解決するためになされたもので、メールを発信する人がメーリングリスト一覧表に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表を管理するサーバの公開鍵さえ入手すれば、メール受信者の数に関係なくメーリングリスト一覧表の運用を容易に行うことができるとともに、メーリングリスト一覧表に所属している人を意識することなく、暗号化メールを利用することができるセキュアメーリングリスト配信方法を提供することを目的とする。

【０００９】また、この発明は、簡単な構成で、メールを発信する人がメーリングリスト一覧表に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表を管理するサーバの公開鍵さえ入手すれば、メール受信者の数に関係なくメーリングリスト一覧表の運用を容易に行うことができ、かつメーリングリスト一覧表に所属している人を意識することなく、暗号化メールを利用することができるセキュアメーリングリスト配信装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、この発明のセキュアメーリングリスト配信方法は、メール本文を使用してメール送信者の電子署名を作成して上記メール本文と電子署名をまとめて共通鍵を使用することにより暗号文を作成するとともに、この共通鍵をメール受信者の公開鍵で暗号化する第１ステップと、上記メール送信者より上記メール受信者に送信された上記暗号化された共通鍵をメール受信者の秘密鍵で復号化するとともに、上記暗号化されたメール本文を復号化された共通鍵により復号化する第２ステップと、上記送信された電子署名を上記メール送信者の公開鍵を用いて復号化するとともに、上記メール本文からメッセージダイジェストを作成する第３ステップと、メーリングリスト一覧表に登録されているユーザのメールアドレスを鍵変換デーモンによりメーリングリスト一覧表から取得し、その取得したメールアドレスから公開鍵を取得して、このメールアドレスと公開鍵を使用して共通鍵を暗号化する第４ステップとを備えることを特徴とする。

【００１１】この発明のセキュアメーリングリスト配信方法によれば、第１ステップでは、メール送信者側においてメール送信者の電子署名はメール本文を使用して作成する。この電子署名とメール本文とから共通鍵を使用することにより暗号文を作成する。この共通鍵はメール受信者の公開鍵で復号化する。

【００１２】次に、第２ステップでは、メール受信者側において、暗号化メール文と暗号化された共通鍵のうち、メール本文の暗号化に使用された共通鍵をメール受信者の秘密鍵で復号化するとともに、上記暗号化したメール本文を復号化した共通鍵を用いて復号化する。

【００１３】次に、第３ステップでは、受信者に送信された電子署名をメール送信者の公開鍵を用いて複合化し、メール本文からメッセージダイジェストを作成する。

【００１４】第４ステップでは、鍵変換デーモンによりメーリングリスト一覧表に登録されているユーザのメールアドレスからメールアドレスを取得する。この取得したメールアドレスから公開鍵を取得する。これらの取得したメールアドレスと公開鍵を使用して、共通鍵を暗号化する。

【００１５】したがって、この発明のセキュアメーリン

グリスト配信方法では、メールを発信する人がメーリングリスト一覧表に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表を管理するサーバの公開鍵さえ入手すれば、メール受信者の数に関係なくメーリングリスト一覧表の運用を容易に行うことができ、かつメーリングリスト一覧表に所属している人を意識することなく、暗号化メールを利用することができる。

【００１６】また、この発明のセキュアメーリングリスト配信装置は、複数のユーザを登録したメーリングリスト一覧表を管理するメールサーバと、上記メールサーバに存在する公開鍵管理サーバと、上記メーリングリスト一覧表に登録される上記複数のユーザのうちの所定のユーザがメール送信者となって上記メーリングリスト一覧表宛に登録する暗号化メールの発信時に上記メーリングリスト一覧表に登録されている上記ユーザのメールアドレスと公開鍵を検索して、メールアドレスと公開鍵を取得するとともに、上記メールサーバの秘密鍵で一時的に共通鍵で再度暗号化して上記複数のユーザが暗号化メールを復号化するために上記複数のユーザに暗号化メールを送信する鍵変換デーモンとを備えることを特徴とする。

【００１７】この発明のセキュアメーリングリスト配信装置によれば、メールサーバにより管理されているメーリングリスト一覧表に複数のユーザを登録しておき、この登録されているユーザのうちの所定のユーザがメール送信者となってメーリングリスト一覧表に対して暗号化メールを発信する。鍵変換デーモンは、メーリングリスト一覧表に登録されているユーザのメールアドレスと公開鍵を検査することにより、該当するユーザのメールアドレスと公開鍵とを取得する。

【００１８】また、メール送信者からのメーリングリスト一覧表宛ての暗号化メールをメールサーバの秘密鍵で一時的に共通鍵を解読する。この共通鍵をメーリングリスト一覧表に登録されているユーザの公開鍵で再度暗号化して、これらのユーザに暗号化メールを送信する。この暗号化メールが送信されたユーザは、自己の秘密鍵を用いて復号化する。

【００１９】したがって、この発明のセキュアメーリングリスト配信装置では、簡単な構成で、メールを発信する人がメーリングリスト一覧表に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表を管理するメールサーバの公開鍵さえ入手すれば、メール受信者の数に関係なくメーリングリスト一覧表の運用を容易に行うことができる。

【００２０】

【発明の実施の形態】次に、この発明によるセキュアメーリングリスト配信方法および装置の実施の形態について、図面に基づき説明する。図１は、この発明によるセキュアメーリングリスト配信装置の第１実施の形態の構成を示すブロック図である。この図１において、点線で囲まれたメールサーバ１０（メーリングリスト一覧表管理サーバ）の部分がこの発明の特徴をなす構成部分である。

【００２１】ユーザ１がメールサーバ１０で管理されるメーリングリスト一覧表１１を使用し、メーリングリスト一覧表１１には、ユーザ１、ユーザ２、ユーザ３……が登録されており、ユーザ１がメール送信者、すなわち、暗号化メールの発行者となって、メーリングリスト一覧表１１に対して暗号化メールを発信する場合を例示している。鍵変換デーモン１２は、メールサーバ１０の中に存在する。鍵変換デーモン１２では、メーリングリスト一覧表１１に属するユーザ２、ユーザ３……のメールアドレスと公開鍵を検索し、必要に応じて公開鍵管理サーバ１３に問い合わせを行い、メールアドレスと公開鍵を取得する。

【００２２】また、メーリングリスト一覧表１１宛の暗号化メールをメールサーバ１０の秘密鍵で一時的に共通鍵を解き、ユーザ２、ユーザ３……の公開鍵で共通鍵を再度暗号化して、ユーザ２、ユーザ３……に暗号化メールを送り出す。ユーザ２、ユーザ３……は、暗号化メールをそれぞれの秘密鍵を用いて復号化する。

【００２３】次に、この発明によるセキュアメーリングリスト配信装置の第１実施の形態の動作について、図２ないし図６のフローチャートに沿って説明する。この動作の説明に際して、この発明によるセキュアメーリングリスト配信方法の第１実施の形態の説明を兼ねることにする。

【００２４】まず、暗号化メールの処理フローについて説明する。図２におけるフローチャートのステップＳ１ではメール本文１４（平文）を使ってメール送信者（図１では、ユーザ１）の電子署名１５を作成する。電子署名１５の作成方法は、図３の電子署名の作成手順を示すフローチャートに沿って説明する。

【００２５】この図３において、メール本文１４をステップＳ２でハッシュ関数を使ってメッセージダイジェスト１６を作成する。次いで、メッセージダイジェスト１６をステップＳ３でメール送信者の秘密鍵１７を用いて暗号化を行うことにより、上記電子署名１５が作成される。

【００２６】ここで、再度図２のフローチャートの処理手順の説明に戻す。この図２において、ステップＳ４でメール本文１４と電子署名１５とをまとめて暗号文１８を作成する。図４は、メール本文１４の暗号文１８の作成処理手順を示すフローチャートである。この図４に示すように、暗号文１８の作成に際して、ステップＳ５でメール本文１４の暗号化には、共通鍵１９が使われる。

【００２７】次いで、このメール本文１４の暗号化に使った共通鍵１９を図２に示すように、ステップＳ６で暗号化して、暗号文２０を作成する。この共通鍵１９の暗号化に際しては、図５のフローチャートに示すように、

共通鍵１９の暗号化は、ステップＳ７でメール受信者の公開鍵２１で暗号化して、復号化された共通鍵２２を作成する。このようにして作成された暗号文２０と復号化された共通鍵２２はメール受信者（たとえば、メールユーザ２）に送信される。

【００２８】以上までの処理は、メール送信者側の処理であるが、次に、メール受信者側（ユーザ２側）の処理について説明する。このメール受信者側の処理において、メール送信者側からメール受信者側に送信されてきた暗号化メール文、すなわち上記暗号文２０と、復号化された共通鍵２２のうち、復号化された共通鍵２２は図２のステップＳ８において、メール受信者の秘密鍵（図示せず）で復号化する。

【００２９】次に、図２に示すステップＳ９において、暗号文２０を上記ステップＳ８の処理で復号化した共通鍵１９を用いて、復号化してメール本文２３（平文）と、電子署名２４を得る。次に、図２に示すステップＳ１０において、電子署名２４をメール送信者の公開鍵を用いて、図６のフローチャートに示すステップＳ１１でメッセージダイジェスト２５を複合化する。また、同時にメール本文２３は図６のフローチャートに示すステップＳ１２でハッシュ関数を使用してメッセージダイジェスト２６を作成する。

【００３０】ここで、二つのメッセージダイジェスト２５と２６が同じであれば、データの改竄がないことが保証される。この発明においては、上記の処理を踏まえてメーリングリスト一覧表１１の処理を追加している。図２のステップＳ８までの処理で得られた情報はステップＳ１３で鍵変換デーモン１２に転送される。

【００３１】この鍵変換デーモン１２は、図２のステップＳ１４でメーリングリスト一覧表１１に所属しているメンバ、すなわち、ユーザ２、ユーザ３……のメールアドレスをこのメーリングリスト一覧表１１から取得して、上記ステップＳ６の処理に戻る。続いて、ステップＳ１５において、上記ステップＳ１４での処理で取得したメールアドレスから公開鍵情報管理サーバ１３などから公開鍵を取得する。

【００３２】上記ステップＳ１４で得たメールアドレスとステップＳ１５で得られた公開鍵を使って、上記ステップＳ６の処理を行う。以降、上記のステップＳ８，ステップＳ９，ステップＳ１０の処理を行う。この第１実施の形態では、共通鍵の部分の鍵のかけ直ししか行っていないため、従来通りの電子署名などの機能は、そのまま効力を失うことなく使うことができる。

【００３３】このように、セキュアメーリングリスト配信および装置による各第１実施の形態では、メーリングリスト一覧表１１の管理しているメールサーバ１０がメーリングリスト一覧表１１宛てに送られてきた暗号化メールに対してメーリングリストの登録者のメールアドレスと公開鍵を検索し、暗号化メールの鍵をかけかえを行うことにより、メールを発信する人がメーリングリスト一覧表１１に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表１１を管理するメールサーバの公開鍵さえ入手すればよくなる。

【００３４】また、通常のメールの場合と同様に、メーリングリスト一覧表１１に誰が入っているのかを意識する必要がなくなり、メーリングリスト一覧表１１に他のメーリングリストが入っている場合なども同様に暗号化メールを使用することができる。

【００３５】次に、この発明による第２実施の形態について説明する。メーリングリスト一覧表１１に所属している人の公開鍵を鍵変換デーモン１２に一括検索させ、メーリングリスト一覧表１１に所属する人の公開鍵をまとめて入手させたり、メーリングリスト一覧表に所属している人全員の公開鍵をメールとともに添付して送り出すといったことも可能となる。

【００３６】

【発明の効果】以上のように、この発明のセキュアメーリングは配信方法によれば、メール送信者の電子署名をメール本文を使用して作成し、電子署名とメール本文とから共通鍵を使用して暗号文を作成し、その共通鍵を暗号化し、その共通鍵の暗号化をメールメール受信者の公開鍵で暗号化し、共通鍵をメール受信者の秘密鍵で復号化し、暗号化したメール本文を復号化した共通鍵で復号化し、受信者に送信された電子署名をメール送信者の公開鍵を用いて複合化し、メール本文からメッセージダイジェストを作成し、鍵変換デーモンによりメーリングリスト一覧表に登録されているユーザのメールアドレス一覧表からメーリアドレスを取得し、取得したメールアドレスから公開鍵を使用して、共通鍵を暗号化するようにしたので、メールを発信する人がメーリングリスト一覧表に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表を管理するサーバの公開鍵さえ入手すれば、メール受信者の数に関係なくメーリングリスト一覧表の運用を容易に行うことができ、かつメーリングリスト一覧表に所属している人を意識することなく、暗号化メールを利用することができる。

【００３７】また、この発明のセキュアメーリングは配信装置によれば、メールサーバにより管理されているメーリングリスト一覧表に登録されているユーザのうちの所定のユーザがメール送信者となってメーリングリスト一覧表に対して暗号化メールを発信し、鍵変換デーモンは、メーリングリスト一覧表に登録されているユーザのメールアドレスと公開鍵を検査することにより、該当するユーザのメールアドレスと公開鍵とを取得し、メール送信者からのメーリングリスト一覧表宛ての暗号化メールをサーバの秘密鍵で一時的に共通鍵を解読し、この共通鍵をメーリングリスト一覧表に登録されているユーザの公開鍵で再度暗号化して、これらのユーザに暗号化メールを送信し、送信されたユーザは、自己の秘密鍵を用

いて復号化するようにしたので、簡単な構成で、メールを発信する人がメーリングリスト一覧表に所属している人の公開鍵を取得していなくても、メーリングリスト一覧表を管理するサーバの公開鍵さえ入手すれば、メール受信者の数に関係なくメーリングリスト一覧表の運用を容易に行うことができる。

【図面の簡単な説明】

【図１】この発明によるセキュアメーリングリスト配信装置の第１実施の形態の構成を示すブロック図である。

【図２】この発明によるセキュアメーリングリスト配信方法および装置の第１実施の形態の全体的動作の流れを説明するためのフローチャートである。

【図３】この発明によるセキュアメーリングリスト配信方法および装置の第１実施の形態によるメール本文からメッセージダイジェストの暗号化と署名化の処理工程を説明するためのフローチャートである。

【図４】この発明によるセキュアメーリングリスト配信方法および装置の第１実施の形態によるメール本文を共通鍵を用いて暗号化する処理工程を説明するためのフローチャートである。

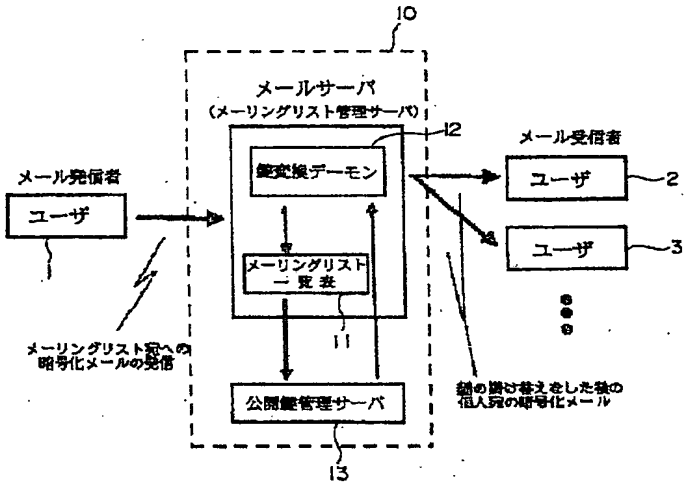
【図５】この発明によるセキュアメーリングリスト配信方法および装置の第１実施の形態による共通鍵の暗号化をメール受信者の公開鍵で暗号化する処理工程を説明するためのフローチャートである。

【図６】この発明によるセキュアメーリングリスト配信方法および装置の第１実施の形態により暗号メール文を共通鍵による複合化と電子署名をメール送信者の公開鍵でメッセージダイジェストを復号化する処理工程を説明するためのフローチャートである。

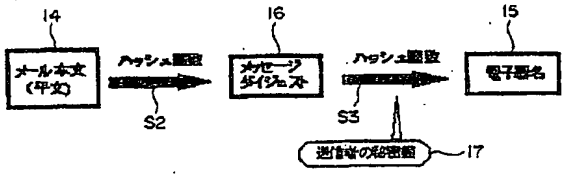
【符号の説明】

１～３……ユーザ、１０……メールサーバ、１１……メーリングリスト一覧表、１２……鍵変換デーモン、１３……公開鍵管理サーバ、１４，２３……メール本文、１５，２４……電子署名、１６……メッセージダイジェスト、１７……メール送信者の秘密鍵、１８，２０……暗号文、１９……共通鍵、２１……メール受信者の公開鍵、２２……復号化された共通鍵、２５，２６……メッセージダイジェスト。

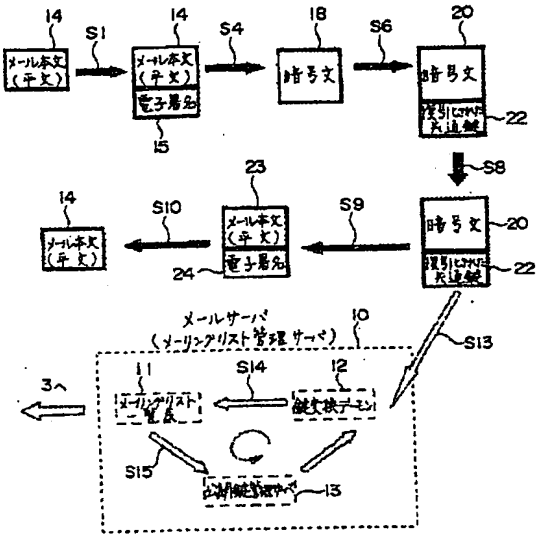
【図１】



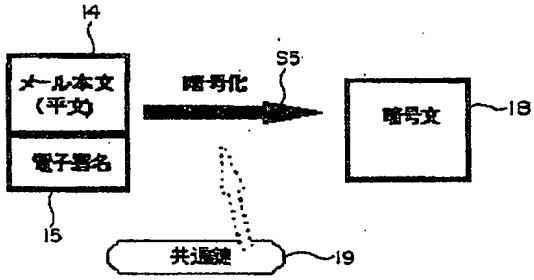
【図３】



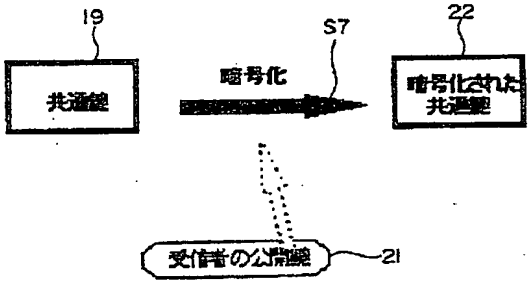
【図２】



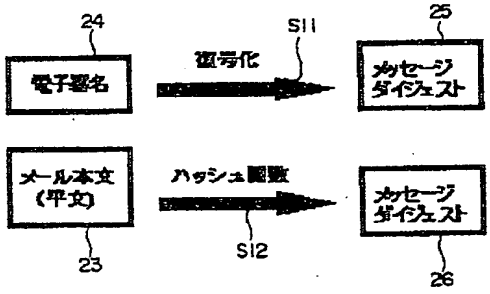
【図４】



【図５】



【図６】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I		テーマコード（参考）
H04L 12/58		H04L 11/20	101B	

Ｆターム(参考)　5B089 GA11 GB03 JA31 JB01 KA13
KB00 KC15 KC57 KE07 KH30
LA01 LA11
5J104 EA19 JA21 LA05 NA02 NA12
PA08
5K030 GA11 GA15 HA06 LA07 LD19
LD20

KM-US-207
IDS

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-124892
(43)Date of publication of application : 28.04.2000

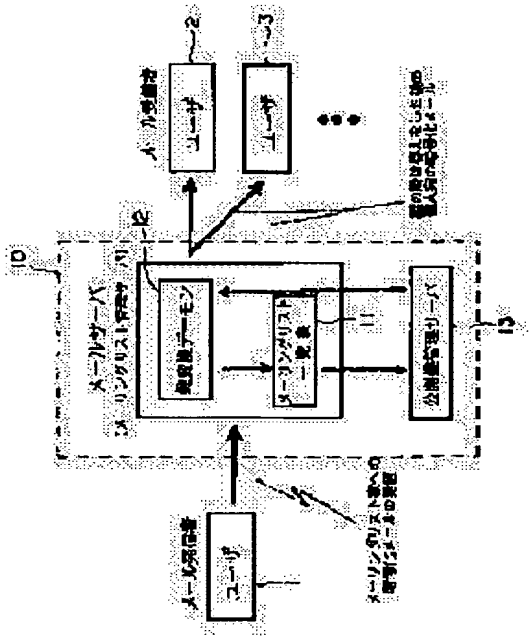
(51)Int.Cl. H04L 9/14
G06F 13/00
G09C 1/00
H04L 9/08
H04L 12/54
H04L 12/58

(21)Application number : 10-294765
(22)Date of filing : 16.10.1998

(71)Applicant : NEC CORP
(72)Inventor : ZAITSU HIDEJI

(54) METHOD AND DEVICE FOR DISTRIBUTING SECURE MAILING LIST

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a secure mailing list distributing device with which a mail transmitter can easily operate a mailing list, regardless of the number of mail recipients only by acquiring the public key of a mail server.
SOLUTION: Users 1-3 are registered on a mailing list 11 managed by a mail server 10, and when the user 1 transmits enciphered mail to the mailing list 11, a key translate daemon 12 retrieves and acquires the mail address and public key of the user 1. To addition, for the enciphered mail addressed from the user 1 to the mailing list, a common key is deciphered by the secret key of the mail server 10, the common key is re-enciphered by the public key of the user 2, the enciphered mail is transmitted to the user 2, and the user deciphers the enciphered mail while using his own secret key.



LEGAL STATUS

[Date of request for examination] 16.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]